نظرية المعلومات وترميز - امتحان أول

Specialization:	Electrical Engineering		Palestinian National Authority Ministry Education & Higher Education Palestine Technical University College of Engineering & Technology
Course Name:	Information Theory and Coding		
Date:	20/03/2011		First Exam Second semester 2010/2011
Time:	11:00-12:00		
Instructor:	Dr. Mutamed Khatib		
Name:	Answer Key	Section:	

Answer *all* the following 4 questions

Q1. *(5 marks)* Consider a source whose statistically independent symbols consist of all possible binary sequences of length k. Assume all symbols are equiprobable. How much information is conveyed on receipt of any symbol?

$$P(x_i) = \frac{1}{M} \qquad L = k \Rightarrow M = 2^k$$

$$H = \sum_{m=1}^{M} P(m) \log_2 \frac{1}{P(m)} = \sum_{m=1}^{M} M \log_2 M = \sum_{m=1}^{M} \frac{k}{M} = M \frac{k}{M} = k$$

$\Rightarrow k$ bits/symbol.

Q2. *(5 marks)* Determine the information conveyed by the specific message $x_1x_3x_2x_1$ when it emanates from each of the following, statistically independent, symbol sources: $M = 4$; $P(x_1) = 1/2, P(x_2) = 1/4$, $P(x_3) = P(x_4) = 1/8$

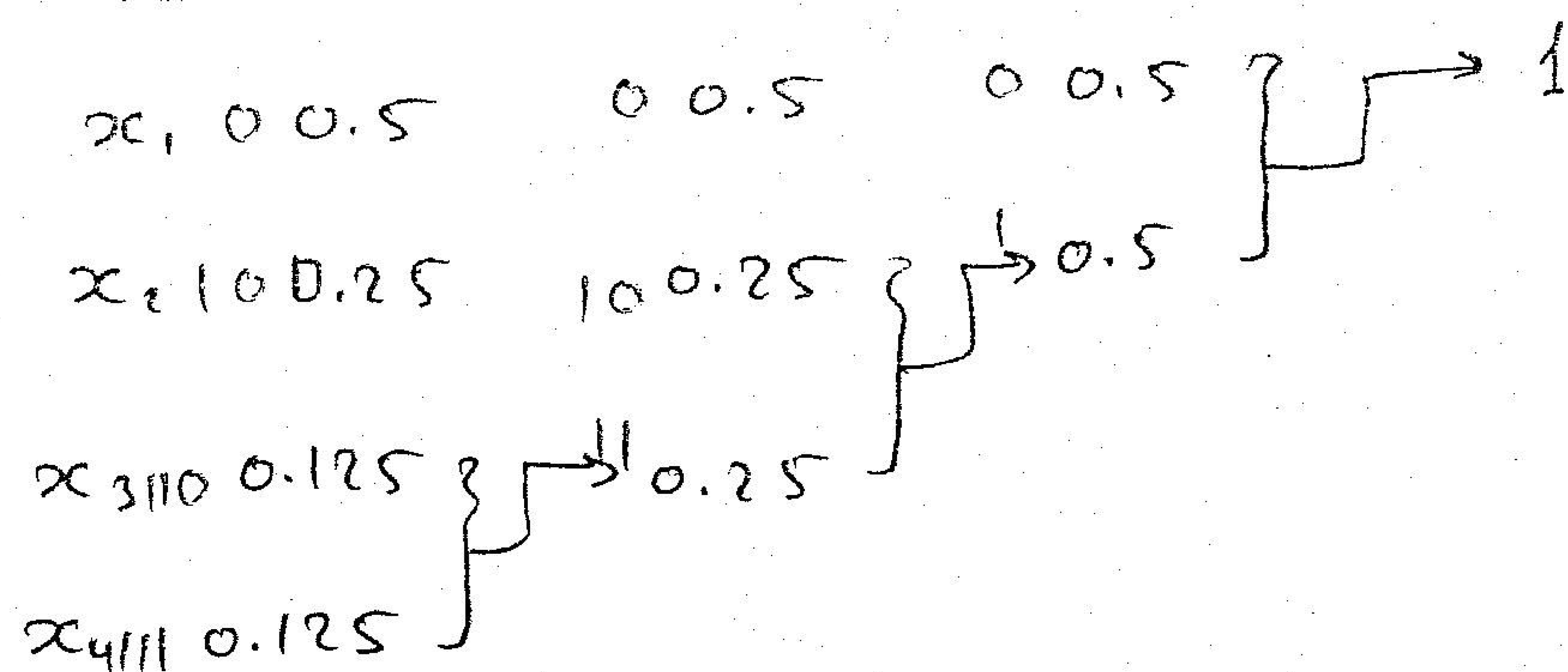
$I_{x_1} = 1$; $I_{x_2} = 2$; $I_{x_3} = I_{x_4} = 3$

$x_1 \; x_3 \; x_2 \; x_1$

$1 + 3 + 2 + 1 \Rightarrow L = 7$ bits

تم الرفع بواسطة
م. معن أبو عيسى

Q3. *(5 marks)* Apply Huffman's code to deduce an optimal code for transmitting the source: $M = 4$; $P(x_1) = 1/2, P(x_2) = 1/4$, $P(x_3) = P(x_4) = 1/8$ over a binary channel.



Q4. *(5 marks)* Use RSA to encrypt the planetext message number 13. Choose the smallest possible values of P and Q. Decipher the resulting ciphertext to check your answer.

$T = 13$ $N = PQ > 13$ $\Rightarrow P = 3$; $Q = 5$ $\Rightarrow N = 15$

$\phi = (P-1)(Q-1) = 2 \times 4 = 8$

factors of ϕ are 1, 2, 4, --

$A = 3$ $\Rightarrow$ remider $\left\{ \frac{3B}{8} \right\} = 1$; 9, 17, 25, 33

$\Rightarrow 3B = 33$ $\Rightarrow B = 11$

$C(13) = T^A \bmod N = 13^3 \bmod 15 = 2197 \bmod 15 = 7$

$T(7) = C^B \bmod N = 7^{11} \bmod 15 = 13$

Good luck